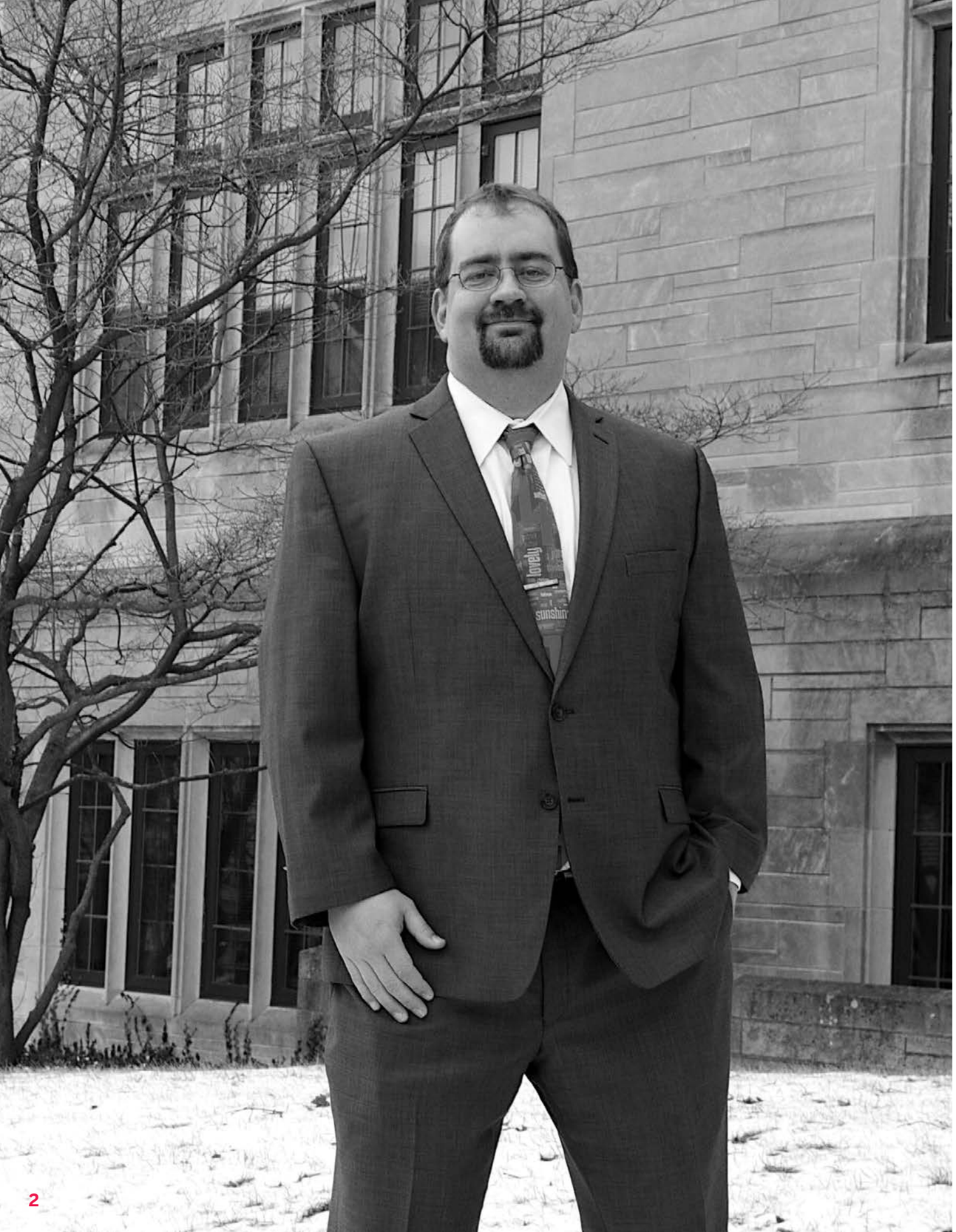
Center for Applied Cybersecurity Research

A PERVASIVE TECHNOLOGY RESEARCH CENTER

2016 Annual Report

Table of CONTENTS



Dear friends of the Center for Applied Cybersecurity Research,

Cybersecurity, with its increasing impact on medical devices, self-driving cars, and our voting process, continues to challenge our society. Over the last year, CACR continued stepping up to this challenge with work bridging research to the real world in a variety of disciplines.

We were honored when the National Science Foundation selected CACR as the lead for its first Cybersecurity Center of Excellence. In this capacity, we are leading groundbreaking work in understanding cybersecurity's role in securing open science—across more than $7 billion dollars of research funded by the NSF, and dozens of NSF-funded projects looking to improve their cybersecurity.

The Crane Naval Surface Warfare Center and CACR are two of Indiana's leading institutions in addressing cybersecurity. We are happy to have signed an agreement this last year to collaborate on cybersecurity. This partnership and exchange of personnel between Crane and CACR will build on the strengths of both organizations to secure some our nation's most critical infrastructure.

Our work in leading the Department of Homeland Security Software Assurance Marketplace (SWAMP) continues to improve the security of the nation's software—which plays an increasing role in our phones, medical devices, and cars. With the release of "SWAMP-in-a-Box" software, organizations can now install onsite software assurance, allowing our work to impact not just open source, but also proprietary and non-public software.

CACR's strengths in bringing together world-class risk and cybersecurity research from Indiana University's School of Informatics and Computing, Kelley School of Business, and the Maurer School of Law, along with its operational cybersecurity expertise and expert staff and fellows, make these highlights possible.

Combined with other activities we describe in this report—our annual Summit in Indianapolis, our new role in helping secure the Open Science Grid, our Speaker Series drawing experts from across the country to IU—these accomplishments demonstrate CACR's continued progress in tackling real-world cybersecurity.

About CACR

The Indiana University Center for Applied Cybersecurity Research (CACR) was established in 2003 to provide the nation with leadership in applied cybersecurity technology, education, and policy guidance. Properly balancing public needs, homeland security concerns, and individual privacy rights is fundamental to CACR's mission.

CACR is distinctive in interweaving research, policy, and operational expertise. The center draws on Indiana University's wide range of scholarly expertise—in computer science, informatics, accounting and information systems, criminal justice, law, organizational behavior, public policy, and other disciplines—and the extensive practical cybersecurity experience of its operational units.

Building on this foundation, CACR has achieved a number of additional successes over the past year:

- Establishing the first "NSF Cybersecurity Center of Excellence"
- Entering into a two-year collaborative agreement with Crane
- Providing cybersecurity expertise to the Open Science Grid
- Launching its healthcare cybersecurity initiative
- Continuing its leadership of the Software Assurance Marketplace (SWAMP)

CACR Applied RESEARCH CYCLE

Application in real-world cybersecurity

Over $16 million in external funding: Lilly Endowment, Inc., National Science Foundation, Department of Energy, Department of Homeland Security, National Institutes of Health, others

Educating, policy, advising

Training via Security Matters, Annual Summit, others; advising Congress, Higher Ed, NSA, DHS, White House, others

Research

Best practices from IU Cybersecurity Research and Operations, and broader community

Mission and VISION

CACR's mission is to advance the state of cybersecurity practice, interdisciplinary research, and understanding in order to serve Indiana University, the state of Indiana, and our national and global communities.

The vision of the CACR is to be a global leader and partner of choice for addressing the multidisciplinary cybersecurity challenges of the modern world.

CACR achieves its mission and vision through collaboration with partners across Indiana University, the state of Indiana, and the nation. To discuss collaboration with CACR on addressing your challenges, contact cacr@iu.edu.

Major IMPACTS

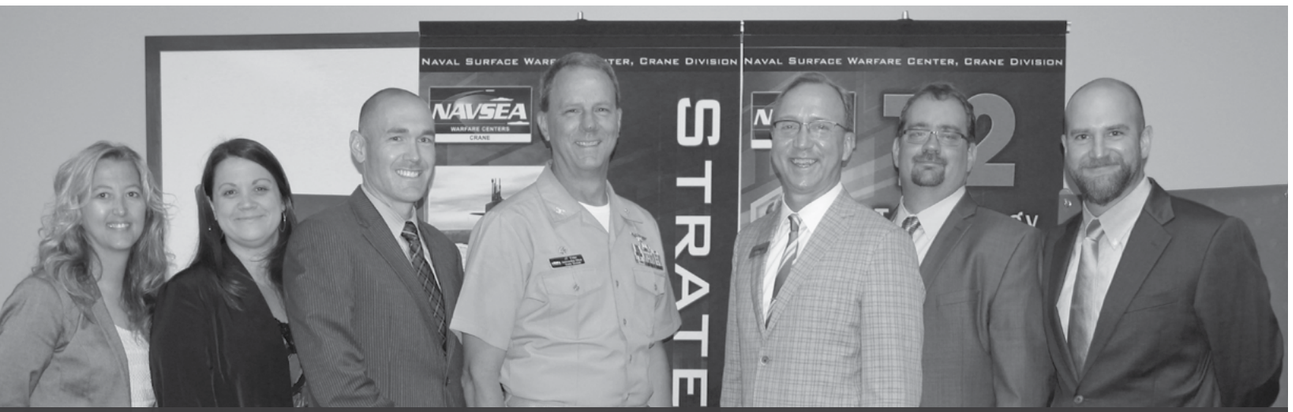
CACR is leading the nation in applied cybersecurity technology, education, and policy guidance. The center had a number of major achievements in the past year.

The SWAMP continues to protect and improve cybersecurity infrastructure

continuousassurance.org

Funded by the Department of Homeland Security (DHS), the SWAMP is a free-to-use, high-performance, centralized cloud-computing platform. It includes an array of open-source and commercial software security testing tools, as well as a comprehensive results viewer to simplify vulnerability remediation.

In the past year, CACR has worked with SWAMP to expand capabilities that broaden support for additional programming languages, and to increase the number and variety of static analysis tools and platforms available to the software assurance community.



CACR collaborates with CRANE on cybersecurity

go.iu.edu/1sBY

In July, CACR entered into a two-year collaborative agreement with the Naval Surface Warfare Center, Crane Division. This agreement, a Cooperative Research and Development Agreement (CRADA), brings together two of Indiana's cybersecurity leaders to share personnel and expertise, and to collaboratively advance research and development in tackling cybersecurity challenges to our nation.

CACR provides cybersecurity expertise to Open Science Grid

opensciencegrid.org

The Open Science Grid (OSG) is a nationwide facility and infrastructure enabling large-scale high-throughput computing for science. In FY16, CACR joined the collaboration, working alongside the IU-based Grid Operations Center to contribute cybersecurity expertise as part of OSG's security team.

CACR establishes first NSF Cybersecurity Center of Excellence

trustedci.org

In 2016, CACR secured a $5 million collaborative grant to lead the first NSF Cybersecurity Center of Excellence (CCoE). This achievement builds on CACR's success leading the Center for Trustworthy Scientific Cyberinfrastructure (CTSC).

The mission of the NSF CCoE is to improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their science endeavors.

CCoE accomplishes this mission through one-on-one engagements with projects to address their specific challenges; education, outreach, and training to raise the state of security practice across the scientific enterprise; and leadership on bringing the best and most relevant cybersecurity research to bear on the NSF cyberinfrastructure research community. Additionally, the CCoE hosts the annual NSF Cybersecurity Summit, bringing the NSF and research communities together to build understanding of the information assets that enable science, while providing a community forum for increasing education, sharing experiences, building relationships, and establishing best practices.

Highlights of the CCoE accomplishments since its inception in January 2016 include:

- Engaged with four **NSF projects**:
    1. **Gemini Observatory** completed an extended CCoE engagement focused on core policy processes and documentation, as well as a close unified look at technical and physical controls at Gemini North.
    2. **Image Based Ecological Information System (IBEIS)** is developing a software platform to collect and share animal data for science and conservation. CCoE collaborated with IBEIS staff to prototype role-based access control for the platform.
    3. **The Array of Things (AoT)** project is, in collaboration with the City of Chicago, developing a network of interactive, modular sensor boxes to be installed around Chicago. CCoE completed a cybersecurity assessment, advising on best practices for developing privacy policy and assisting with incorporating feedback on the draft policy.
    4. **SciGaP** is developing a set of core infrastructure services to support science gateways. CCoE and SciGaP collaborated on the security and identity management functionality of those services.
- Developed an **Open Science Cyber Threat Profile** in collaboration with ESnet and a working group of leaders from the open science community.
- Initiated a **Situational Awareness service** for the NSF community.
- Launched the **CCoE Webinar Series** with two webinars drawing over 30 attendees from the community.
- Developed a condensed **Cybersecurity Training program** targeted at small to medium-sized NSF projects at Indiana University.

Educating the nation on CYBERSECURITY

CACR Speaker Series draws experts from across the country

cacr.iu.edu/events/index.php

Held at least monthly at IU Bloomington, CACR's Security Seminar Speaker Series invites cybersecurity professionals from all over the country to give talks on their individual areas of expertise. These talks are open to all interested students, faculty, and staff, and are offered at IUPUI via live stream.

The 2015-2016

Speaker Series featured the following experts speaking on a range of topics:

Stacy Prowell
Oak Ridge National Laboratory
Let's Instrument Everything and Trust It.

Sadia Afroz
University of California, Berkeley
Challenges of Anonymous Communications

Bart Miller
University of Wisconsin
Why Johnny and Janie Can't Code Safely: Bringing Software Assurance to the Masses

Abhi Shelat
University of Virginia
Micropayments for Decentralized Currencies

Kathryn Seigfried-Spellar
Purdue University
The Authur Pendragon Threat Case Study

Lujo Bauer
Carnegie Mellon University
Towards More Secure and Usable Text Passwords

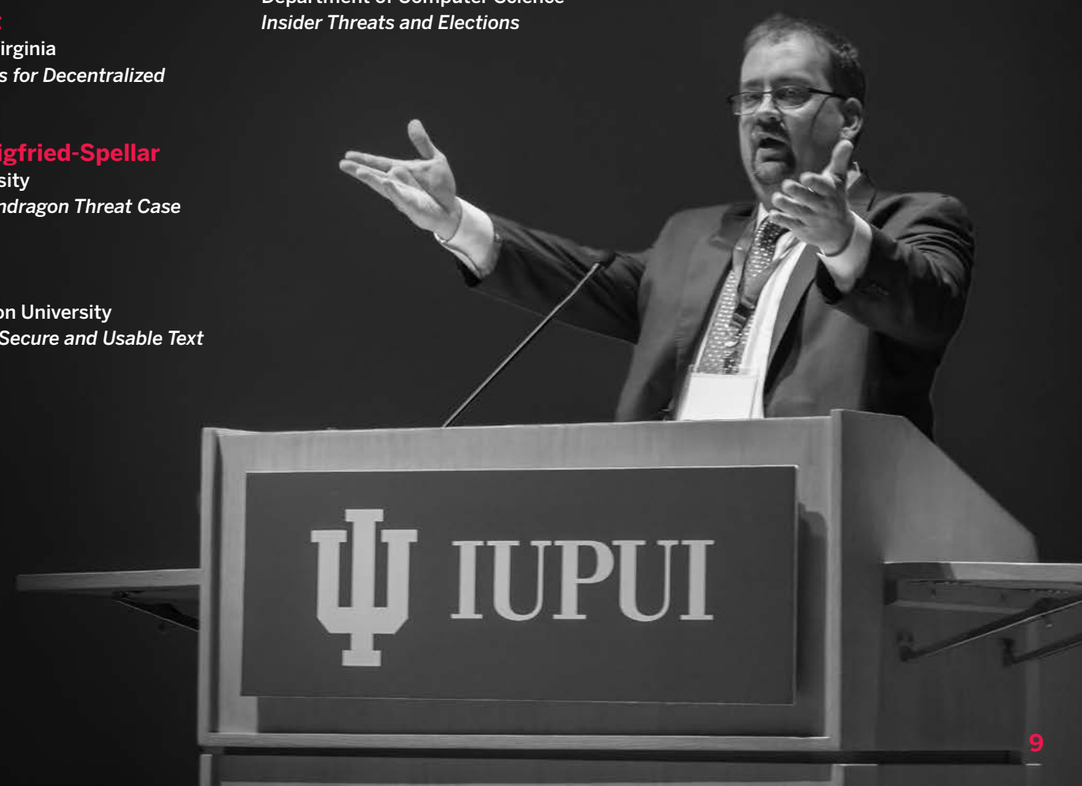
Serge Egelman
International Computer Science Institute
University of California, Berkeley
Making Privacy Decisions in Ubiquitous Computing Environments

Dr. LeAnn Adams Miller
Sandia National Laboratories
Cybersecurity at Sandia National Laboratories

Matt Bishop
University of California, Davis
Department of Computer Science
Insider Threats and Elections

Dr. Yang Wang
Syracuse University
School of Information Studies
From Accessible Authentication to Inclusive Privacy and Security

Adam Slagell
National Center for Supercomputing Applications
Semantically-Aware Network Security Monitoring at Scale with the BRO Platform



Educating the public

CACR is regularly approached by the press to provide comments or background information regarding cybersecurity. As part of its commitment to educating the public, CACR staff readily fulfills media requests, sharing expertise while filling a critical role in raising awareness of cybersecurity issues. In the last year, the center and/or CACR staff and fellows have been featured in the media no less than 100 times.

CACR brings together leaders in cybersecurity from across the country. The center has continued to work as a connection between operational, practical, and academic communities.

NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

trustedci.org/2016summit

Through leadership of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC), CACR has planned and executed the NSF Cybersecurity Summits for Large Facilities and Cyberinfrastructure for the past three years.

The NSF cyberinfrastructure ecosystem presents an aggregate of complex cybersecurity needs (e.g., scientific data and instruments, unique computational and storage resources, complex collaborations) as compared to other organizations and sectors. This community has a unique opportunity to develop information security practices tailored to these needs, breaking new ground on efficient, effective ways to protect information assets while supporting science.

With 90 attendees from 50 NSF-funded programs (including 14 large facilities), the Summit brings together leaders in NSF cyberinfrastructure and cybersecurity. Attendees annually work toward building a trusting, collaborative community, and seriously addressing the community's core cybersecurity challenges. At least one NSF solicitation has made attendance, viewed as critical to cybersecurity, a mandatory component.

CACR Cybersecurity Summit

cacr.iu.edu/events/cybersecurity-summit/index.php

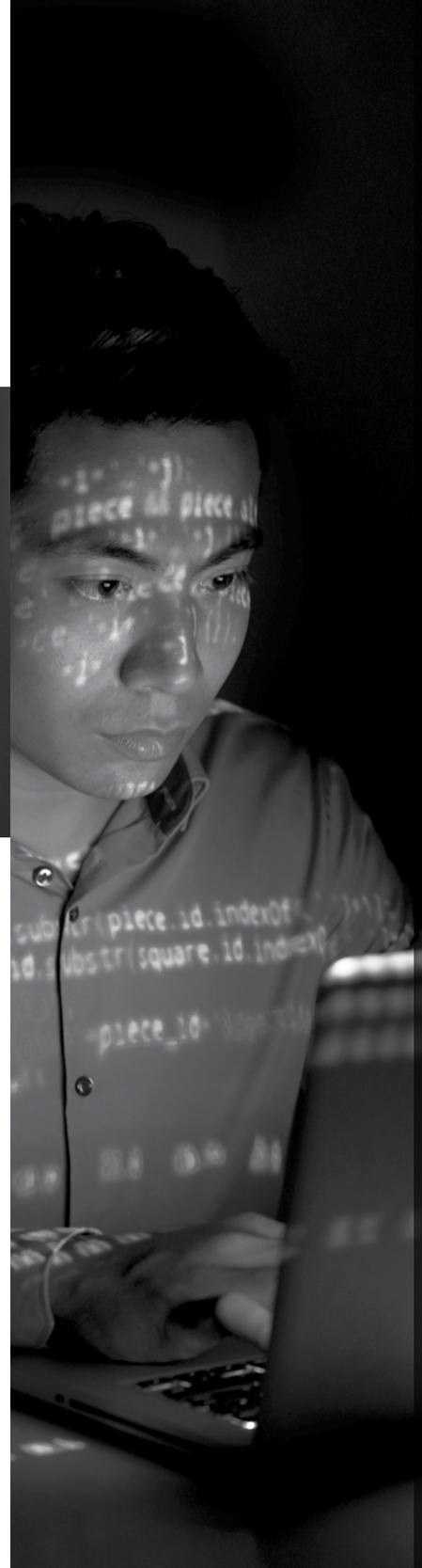
Since 2010, CACR has brought together leading visionaries in the areas of applied cybersecurity technology, education, and policy at an annual Cybersecurity Summit. During this one-day event, attendees discuss the proper balance of public needs, homeland security concerns, and individual privacy rights.

The 2015 CACR Cybersecurity Summit focused on privacy and risk management, and featured keynotes from NIST's Ron Ross and the ABA Cybersecurity Legal Taskforce's Harvey Rishikof. Attendees totaled 180, representing 73 organizations and institutions such as Raytheon, Indiana Department of Homeland Security, University of Kentucky, Indiana Office of Technology, Barnes & Thornburg, Purdue University, Eli Lilly, and the Indiana Economic Development Corporation.

A strong focus on
ADVANCING OUTREACH EFFORTS

CACR's work often focuses on security challenges in context. This is done through outreach with the various communities the center serves. In the past year, some of the most impactful outreach has been:

- **National Security Ethics Workshop:** In November 2015, CACR co-sponsored a visit from U.S. Army War College's Dr. Leonard Wong. Dr. Wong participated in an "Ethics for Breakfast" event with undergraduate students, a faculty workshop on "Ethics, Leadership, and National Security," and a public lecture "Societal Trust in the Military."
- **Everyday Cybersecurity:** In May 2016, CACR presented "Everyday Cybersecurity" to the Electronics Representatives Association of Indiana and Kentucky. This presentation, directed at small and medium business owners, provided attendees with easy to implement measures to make their lives and businesses significantly more secure.
- **IT Security Training for Lawyers:** In December 2015, CACR held training, entitled "Practical Cybersecurity for Lawyers and Law Firms," for lawyers at Barnes & Thornburg. This training focused on increasing literacy and perspective around cybersecurity; providing specific, practical, actionable guidance; and helping attendees develop the know-how to get technical expertise when they need it.
- **Practical Cybersecurity for Open Science Projects:** Held in April 2016, this CACR-led training addressed information security requirements outlined in NSF Major Research Equipment and Facilities Construction / Large Facility cooperative agreements, providing guidance, tools, and resources for open science projects of all sizes.



CACR leads creation of cybersecurity.iu.edu

CACR led the development of the Cybersecurity at IU website, a repository for information regarding cybersecurity at Indiana University. Representing the university's comprehensive approach to exploring the new frontier of cybersecurity, the site is a collaborative effort between CACR, the School of Informatics and Computing, the Kelley School of Business, the Maurer School of Law, Public Safety and Institutional Assurance, and REN-ISAC.

CACR focuses on the next generation

CACR held its inaugural Security Matters Cybercamp for high school students from Bloomington, Indianapolis, and New Albany. CACR launched the camp to address the need for cybersecurity outreach and education for K-12 students. The camp's purpose is to educate youth about the importance of online security and privacy matters, equip them with tools and knowledge to protect against cyber crime and cyber threats, and show them what being a cybersecurity professional can look like—all while addressing the need to build the pipeline of young professionals into the field.

CACR helps secure protected health information end to end

CACR launched its healthcare cybersecurity initiative this past year by assuming responsibility for HIPAA consulting services for University Information Technology Services. Designed to help organizations secure patient health information end to end, the new services use a more comprehensive approach that weaves cybersecurity into user workflows. CACR leverages the widely used NIST risk management framework, which allows organizations to address HIPAA and FISMA compliance simultaneously.

During the past year, CACR has provided HIPAA guidance to national labs, supercomputer centers, and universities—but its largest impact has been at home. CACR raised healthcare cybersecurity across Indiana University by helping achieve or maintain HIPAA compliance for central systems that store protected health information for the IU Schools of Medicine, Dentistry, Nursing, and Optometry. These include 41 systems managed by the UITS Client Services and Support, Enterprise Systems, Learning Technologies, Networks, and Research Technologies divisions.

CACR also engaged in over 100 HIPAA consultations and collaborative projects with the Indiana Clinical and Translational Sciences Institute; trained over 350 IT staff on the HIPAA Security Rule; delivered a presentation on HIPAA compliance at the Statewide IT Conference; and offered a risk management course for Indiana University users at large.

Leadership

CACR Director **Von Welch** has more than a decade of experience developing, deploying, and providing cybersecurity for private and public sector HPC and distributed computing systems.

Senior Fellow and Founding Director **Fred H. Cate** specializes in information security law and policy issues and is routinely called upon to testify before congressional committees; speak before professional, industry, and government groups; and comment on cybersecurity-related stories in the news.

Associate Director **William Barnett** is the Indiana CTSI and Regenstrief chief research informatics officer.

Associate Director **Mark Bruhn** is Indiana University's associate vice president for assurance and public safety.

Associate Director **Scott Orr** is an instructor in Network Security and System Administration at IUPUI.

Administrative Director **Leslee Cooper** has over two decades of accounting and financial management experience.

Staff

CACR staff help oversee daily operations such as administrative, management, and external relations support, as well as security and policy analysis.

Diana Borecky,
Senior Administrative Assistant

Randy Heiland,
Senior Systems Analyst/Programmer

Craig Jackson,
Chief Policy Analyst

Ryan Kiser,
IT Specialist

Mark Krenz,
Lead Security Analyst

Sarah Portwood,
Executive Assistant to Fred H. Cate

Zalak Shah,
Systems Analyst

Anurag Shankar,
Senior Security Analyst

Susan Sons,
Senior Systems Analyst

Amy Starzynski Coddens,
Education, Outreach and Training Manager

Fellows Program

CACR has a dozen fellows, each bringing unique insights and connections to the center, allowing it to capitalize on the interdisciplinary strengths of Indiana University and the broader community. Fellows represent a wide range of perspectives, including law, policy, ethics, and informatics.

Fred H. Cate, Maurer School of Law
L. Jean Camp, School of Informatics and Computing
Jake Chen, School of Informatics and Computing (IUPUI)
Arjan Durress, Department of Computer and Information Science (IUPUI)
David P. Fidler, Maurer School of Law
Apu Kapadia, School of Informatics and Computing
Steven Myers, School of Informatics and Computing
Scott J. Shackelford, Kelley School of Business
Robert Templeman, Naval Surface Warfare Center, Crane Division
Joseph Tomain, Maurer School of Law
Xiaofeng Wang, School of Informatics and Computing
Xukai Zou, Department of Computer Science (IUPUI)

Acknowledgment

CACR is a research center affiliated with the Indiana University Pervasive Technology Institute and a member of the Indiana University cybersecurity community. CACR's work is funded by the IU Office of the Vice President for Information Technology, the IU Office of the President, the Department of Homeland Security, and the National Science Foundation (grants 1547272, 1234408, 1228668, and 1642070). None of the opinions expressed in this report should be taken to represent the opinions of funding entities.

CENTER FOR APPLIED CYBERSECURITY RESEARCH

2719 E. 10th Street, Suite 231, Bloomington, IN 47408 | cacr@iu.edu | (812) 856-8080